STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

ARMY KNOWLEDGE MANAGEMENT (AKM): CHALLENGES AHEAD

BY

LIEUTENANT COLONEL JACKIE J. BRYANT
United States Army

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

ARMY KNOWLEDGE MANAGEMENT (AKM): CHALLENGES AHEAD

by

Lieutenant Colonel Jackie J. Bryant
United States Army

Mr. David Birdwell
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Jackie J. Bryant

TITLE: Army Knowledge Management (AKM): Challenges Ahead

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 34 CLASSIFICATION: Unclassified

Challenges exist in the areas of information technology and knowledge sharing throughout the Army. Organizations have tremendous amounts of information on computers but find it hard to share the information or knowledge outside of their community. Army Knowledge Management (AKM) is the answer to this challenge and provides the Army strategy to transform itself into a network-centric, knowledge-based force. AKM is an integrated, systematic approach to identifying, managing, and sharing virtually all of the Army's information assets, including databases, documents, policies and procedures, as well as previously unarticulated expertise and experience resident in individual workers.

This paper centers on the problem of knowledge sharing and the protection of information networks in the Army. It begins with the challenges we face today in the areas of information technology and knowledge sharing. It reiterates knowledge sharing in our senior leadership's strategies, joint visions, and quadrennial review. It covers the importance of learning from our commercial industry counterparts. It communicates the Army's leadership vision, involvement, purpose, and goals of AKM. Finally, the paper addresses the challenges and recommended solutions for knowledge sharing and the protection of information networks through information assurance (IA).

TABLE OF CONTENTS

PREFACE

Mr. David Birdwell, COL Glenn Trimmer, COL Tom Gannan, and Mr. Tom Wagner reviewed different sections of this manuscript and made constructive suggestions. Without their assistance, the text could not have reached its present shape. I truly appreciate their assistance in helping me toward success. Last, but not least, I want to thank my wonderful wife, Joanie, for being so patient and supportive during this endeavor. As always, I am truly blessed and grateful for her moral support and help.

LIST OF ILLUSTRATIONS

ARMY KNOWLEDGE MANAGEMENT (AKM): CHALLENGES AHEAD

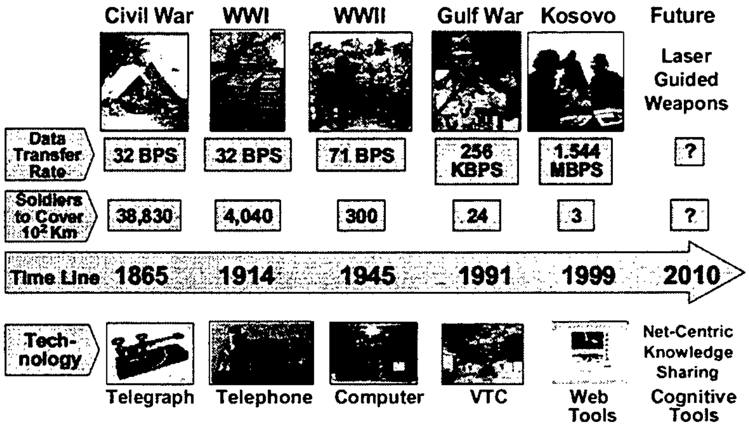
> "The government depends on what it knows. Or to be more specific -- on what it knows, how it uses what it knows, and how fast it can know something new. For just this reason, the Federal community is turning to the growing field of Knowledge Management. "
>
> —Jon Desenberg
> GSA Office of Knowledge Management

On the morning of September 11, 2001, America suffered its worst terrorist attack in history. As thousands of innocent citizens and military personnel began their business day, four planes left Boston, Washington, and Newark, bound for California, and were hijacked. Until that day, few thought of commercial aircraft as weapons of mass destruction. The first two hit and destroyed the World Trade Center in New York City, two of the tallest buildings in the world, symbol of our nation's industry and pride, and the daily workplace of thousands of citizens. The third plane plunged into the Pentagon, the seat of our nation's military power, and the daily workplace of more than 20,000 military, DoD civilians, and contractors. The fourth plane went down in Pennsylvania – miles short of its target, reportedly thanks to the bravery of passengers. Thousands of lives changed forever within the space of two hours as husbands and wives, fathers and mothers, sons and daughters, brothers and sisters would never see one another again. The attacks were clearly a deliberate effort to cripple the morale of America, shaking our faith in our safety and our belief in our strength. It was an attack on our nation's political, economic, informational, and military elements of power. The question arises, could our government have prevented these attacks by providing the right information, at the right time, in the right form, assured and secure, and to the right people? For the Army, AKM may be the enabler to help accomplish this task.

TODAY'S PROBLEMS WITH INFORMATION TECHNOLOGY AND KNOWLEDGE SHARING

Technology has changed the way our nation's military conducts war on the battlefield. We live in an age of information technology and information exchange. Figure 1 depicts the communications technology of choice, data transfer rates, and the number of soldiers that occupied ten square kilometers of space on the battlefield from the Civil War era to 2010. The figure clearly shows an information age "boom" over the past one hundred and thirty-six years. Even though this information age "boom" helps our nation and military in many ways, problems exist in the area of information technology and knowledge sharing at Headquarters, Department of the Army, Major Commands (MACOMs), installations, and tactical units.

These organizations are centric. In other words, they have a tremendous amount of information on computers but find it hard to share the information outside of their community. Information is very difficult to find, access, and validate. Email servers, personal computers, local area networks, and wide area networks number in the thousands Army wide. Organizations purchase thousands of software licenses per year at tremendous cost. Locally generated Web sites are unique and computer memory intensive. Computer hardware and software systems are not compatible or interoperable. The purchase of information structure is piecemeal which causes a significant lag time in completion of the structure needed to pass the information. Technology standardization does not exist from installation to installation and the installation Directors of Information Management (DOIMs) work independently. The above uncoordinated efforts cost the Army a tremendous amount of money each year in the area of information technology.



BPS: Bits per second KBPS: Kilobits (1024) per second VTC: Video Tele-Conferencing

FIGURE 1 – COMMUNICATION DEVICES, DATA TRANSFER RATES, AND SOLDIERS

To promote peace, prepare for war, and dominate the battlefield, we must obtain information superiority and shared knowledge. Our senior leadership has laid out the strategy, visions, and reviews that set us on the journey to KM. It is important to cover these documents, in short, to set the stage for where we are and where we are going in the future with KM.

JOINT VISION, MILITARY STRATEGY, AND QUADRENNIAL REVIEW

Former Chairman of the Joint Chiefs of Staff, General John M. Shalikashvili emphasized in both Joint Vision 2010 (JV2010) and the National Military Strategy (NMS) the importance of information superiority. Even though the dates on these documents date back to 1996 and 1997 respectively, they communicate the guidance in terms of a joint vision and strategy to the services. The message to the services was to get coordinated on their approaches to warfare in the area of information technology and exchange. JV2010 states that information superiority is "...the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same".[1]

All commanders need accurate, uninterrupted, and timely information to train for war in peacetime and win the nation's wars when called to do so in conflict. The NMS supports the JV2010 by stressing that information superiority "...yields battlespace awareness, an interactive, shared and highly accurate picture of friendly and enemy operations as they occur. Information superiority allows our commanders to employ widely dispersed joint forces in decisive operations, engage and reengage with the appropriate force, protect the force throughout the battlespace, and conduct tailored logistical support."[2] The ability to gather, process, and disseminate an uninterrupted flow of reliable and precise information under any conditions is a great strategic and military advantage.

Joint Vision 2020, JV2010's successor, reiterates information superiority and labels it as an essential enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control. Information superiority provides increased information at all levels of command, which translates into knowledge sharing. "Information superiority provides the joint force a competitive advantage only when it is effectively translated into superior knowledge and decisions. The joint force must be able to take advantage of superior information converted to superior knowledge to achieve "decision superiority" – better decisions arrived at and implemented faster than an opponent can react, or in a noncombat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission."[3]

The most current document that builds upon the importance of shared knowledge is the 2001 Quadrennial Review (2001 QDR). The Secretary of Defense, Donald H. Rumsfeld, wants to make sure that DoD leverages information technology and innovative concepts to develop interoperable Joint C4ISR. The success of future joint, civilian, and coalition operations rests upon the importance of sharing timely information. "The effectiveness of these operations will depend upon the ability of DoD to share information and collaborate externally as well as internally."[4] The 2001 QDR states that we have networked connectivity and incredible amounts of information, but our business practice of sharing information is delinquent; we need to find innovative ways in the future to share information to better the entire DoD. "The Department's financial and non-financial operations and systems do not work together effectively to produce the most desirable business management information. Correcting this deficiency will require a broad set of initiatives."[5]

The message in the above strategies, visions, and review spell out change in the way we share knowledge in peacetime and war. The management of knowledge or information over networked systems is the way ahead for not only the Army but also the entire DoD. However, how do we change? How can we learn? The Army must learn and capitalize on implementation lessons from the commercial world in the area of KM. The next section briefly points out the importance of the commercial world's influence in driving technology and knowledge sharing around the globe. The section ends with one example of a successful company that has harnessed technology and innovative ways of sharing knowledge.

THE COMMERCIAL WORLD'S INFLUENCE ON KNOWLEDGE MANAGEMENT

"Often in the past, military organizations pioneered both the development of technology and its application; such is not the case today. Major advances in information technology are being driven primarily by the demands of the commercial sector. Furthermore, information technology is being applied commercially in ways that are transforming business around the globe."[6]

Successful organizations are those that are information enabled. They have found ways to leverage the available information, make the right decisions, produce the products that are in demand, and perform these processes efficiently. The lessons learned in the commercial world are not all great ideals, but should be used as inputs to our concepts and development processes. If we ignore the lessons learned in the business world, we deny ourselves an opportunity to learn from the experiences of others when they are applicable to warfighting. The ability to share information across functional areas enables a decision maker to make decisions that maximize value from an overall organization perspective rather than a purely functional perspective. The following is an excerpt from the book *Network Centric Warfare,* which shows how Wal-Mart harnessed technology, information superiority, and KM.

> Wal-Mart is the recognized leader in the transaction-intensive retail sector, and uses information superiority to create a competitive advantage by adding information to retailing to achieve precision retailing. Wal-Mart's superior competitive position resulted from reducing distribution costs. This required the co-evolution of organization and process, plus an information infrastructure consisting of a sensory capability and semi-automated transaction capabilities. The sensors include point of sales scanners that collect information on the 90 million (on average) transactions that take place each week. Sharing this information with suppliers in near real time enables suppliers to optimally control production and distribution, as well as manage their individual supply chains. In the words of Jack Welch, the CEO of General Electric: When Wal-Mart sells a light bulb on the register, it goes to my factory instantly—I [General Electric] make the bulb for the one they just sold. When the decision was made to share information directly with suppliers, costs were reduced and performance increased. A high level of awareness is generated at each Wal-Mart store by fusing real-time information with historical and environmental information. Sales statistics for each of the 100,000-plus products are generated on a store-by-store basis, permitting department managers in each Wal-Mart store to compare daily

> sales figures with historic sales figures from the previous day, the previous week, and the same periods the previous year. In addition, each department manager is able to determine in real time existing inventory levels, the amount of product in transit (in-transit visibility), and inventory levels at neighboring Wal-Mart stores. This very high level of awareness enables local section managers to identify opportunities in near real time and take appropriate action to increase sales and revenues. Superior competitive awareness enables Wal-Mart to suppress costs, increase sales, and improve net earnings.[7]

The above lesson learned from Wal-Mart is a great example of success and could be used in the Army's own logistical system. The next section will cover the importance of essential Army senior leadership vision and involvement in the AKM process and implementation.

THE IMPORTANCE OF ARMY SENIOR LEADERSHIP VISION AND INVOLVEMENT

> "Sharing information and getting good feedback needs to be encouraged. We need to undergo change to adapt and become a knowledge-based, learning organization."
>
> General John M. Keane
> Vice Chief of Staff, US Army

General Shinseki, the Army's senior strategic leader, sees information management and technology as a very important undertaking and an integral part of transformation. He tasked the Director of Information Systems for Command, Control, Communications, and Computers (DISC4) in the Army Transformation Campaign Plan with the following: "...coordinate the development of operational and support C4ISR architecture products required to develop a systems architecture and to support force development events for the Interim Force and the subsequent Objective Forces. Ensure all digitally capable materiel is fully operational, compatible, and interoperable before providing such materiel to the units."[8]

The message is change the culture of information technology and exchange in the Army, and the new title for change in the information area is AKM. AKM is defined as an "...integrated, systematic approach to identifying, managing, and sharing all of the Army's information assets, including databases, documents, policies and procedures, as well as previously unarticulated expertise and experience resident in individual workers."[9]

AKM transformation is not just an end state but a journey to an established goal or objective for the good of the overall Army. The DISC4 and the Signal Corps' strategic leadership face many challenges on the journey of transformation and KM. Before any transformation can take place, a senior leader develops and communicates a clear vision.

A vision statement gives an organization direction towards a future objective or goal. The vision helps spell out the journey and provides a desired end state. In the past, strategic leaders often wrote visions in a vacuum; that is, members of the organization had no or little input to the written vision. In addition, strategic leaders failed to communicate the vision to the people within their organizations. Furthermore, visions were wordy, unclear, and all too often force-fed to organizations. This resulted in stovepipe systems throughout the Army that included personnel and communications technologies. Many of these systems could not communicate and operate with each other, thus the legacy force.

The Signal Corps needed a clear vision in helping the Army move toward the objective force of high technology and KM. We can not afford to produce a vision statement in a vacuum and force stovepipe systems on the Army. We need to develop a vision process that the community is a part of and will accept. LTG Peter M. Cuviello, DISC4 and the Army's Chief Information Officer (CIO) is just one of many General Officers who make up the Chief of Staff of the Army's (CSA) transformation team. LTG Cuviello is the point man for the Signal Corps strategic leadership and crafted the following vision statement that supports the transformation plan: "The Army's strategic change agent for world class network centric knowledge based capabilities enabling transformation to assure war fighting dominance... this decade."[10]

The vision is by no means magic, and the objective force will not come from the "magician's hat." The vision communicates that change is necessary in the C4 community to support war-fighting dominance in this decade. A huge challenge in the Army today is how to change the way we share and manage information. So, where are we today in terms of sharing information? We are in a position of much needed improvement. The goal of the strategic leader in this case is to change the information sharing culture.

To ensure that everyone in the Army is aware of the CSA's transformation objective in the area of C4ISR and KM, LTG Cuviello has communicated the following AKM vision statement. "A transformed Army, with agile capabilities and adaptive processes, powered by world class net-centric access to knowledge, systems, and services, interoperable with the Joint environment."[11] The AKM vision received the stamp of approval from General Shinseki on February 15, 2001 at a 4 Star Commander's Conference.[12] This definitely shows that the strategic leadership supports the change in the information technology culture and sets the stage for the conceptual framework for the Army's AKM strategic plan. Figure 2[13] depicts the AKM framework that makes up the knowledge based organization as a whole. As the figure shows, cultural change is prevalent in the areas of people, policies, and information technology.

The next section will build upon this AKM framework by addressing the Army's AKM strategic plan and goals.

THE ARMY'S AKM STRATEGIC PLAN

The purpose of this plan "...is to establish the Army as a knowledge-based organization through a strong KM program using robust information technology and the intellectual capital of its people and systems to enable the timely transfers of knowledge anywhere, anytime. As such, this plan defines KM and outlines a framework and strategy for managing the Army's knowledge assets and resources."[14] On August 8, 2001, the Secretary of the Army and the CSA sent out a memorandum to the entire Army, which list the five main goals that comprise the Army's KM vision and purpose. The memorandum reiterates the importance of Army leadership working together to achieve the enterprise AKM goals in support of Army Transformation. The Secretary and CSA state that "This effort is an integral part of Army Transformation. AKM is intended to improve decision dominance by our warfighters and business stewards – in the battlespace, in our organizations, and in our mission processes."[15] The main goals give direction from the Army senior leadership, assign responsibilities, and establish timelines for the MACOMs. These goals spell out major cultural changes in the way the Army will conduct business in the future.

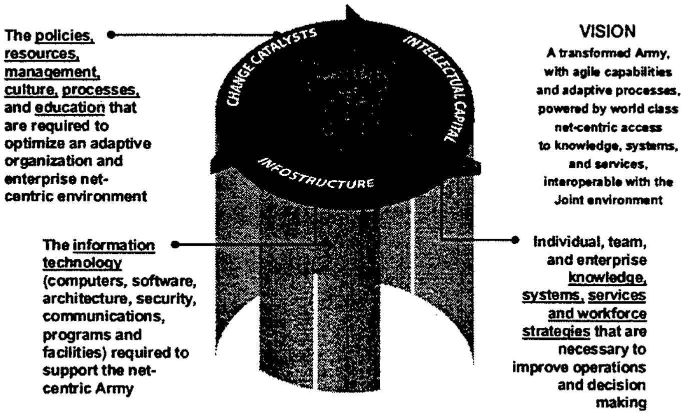

The policies, resources, management, culture, processes, and education that are required to optimize an adaptive organization and enterprise net-centric environment
CHANGE CATALYSTS
INTELLECTUAL CAPITAL
INFOSTRUCTURE
VISION
A transformed Army, with agile capabilities and adaptive processes, powered by world class net-centric access to knowledge, systems, and services, interoperable with the Joint environment
The information technology (computers, software, architecture, security, communications, programs and facilities) required to support the net-centric Army
Individual, team, and enterprise knowledge, systems, services and workforce strategies that are necessary to improve operations and decision making

FIGURE 2 – ARMY KNOWLEDGE MANAGEMENT FRAMEWORK

Goal 1 – Adopt governance and cultural changes to become a knowledge-based organization. New policies, management structures, and strong leadership at all echelons will be necessary to manage knowledge and infostructure at the enterprise level. To achieve this, we have tasked the Army CIO to lead change across a broad spectrum of AKM goals. Effective October 1, 2001, all MACOM information technology (IT) initiatives, other than those that are centrally managed acquisition programs, will be reviewed by the Army CIO Executive Board. MACOM automation funds programmed for IT efforts will be withdrawn from the MACOMs and centrally managed. MACOMs will take immediate action to curtail IT investments unless they have a waiver and funding from the Army CIO. Further, MACOMs will request waiver and funding authority, in concert with Goals 3 and 4 of the AKM Strategic Plan, from the Army CIO.

Goal 2 – Integrate knowledge management and best business practices into Army process. We will establish collaborative work environments and find

> innovative ways of doing business to improve Army decision making and operations. We will find ways to share information across boundaries and apply breakthrough thinking so that we achieve greater performance and enterprise cohesion in our activities. In this regard, MACOMs will provide the Army CIO, by October 1, 2001, a summary review of your knowledge management initiatives, best business practices, and plans to achieve data sharing along with your point of contact, so that we can begin to share and capitalize on these as an enterprise.
>
> **Goal 3 – Manage the infostructure at the enterprise level.** By October 1, 2001, we will designate a single authority to operate and manage the Army's infostructure at the enterprise level. In the meantime, MACOMs will report their infostructure baseline and consolidation initiatives (ongoing and planned) to the Army CIO by September 10, 2001. We will implement our enterprise consolidation strategy, using the Military District of Washington (MDW) as our first phase, by February 1, 2002. We will consolidate all Army infostructure in accordance with the enterprise consolidation strategy and lessons learned from the MDW by October 1, 2002. The Army CIO will provide the draft enterprise strategy by November 1, 2001, and MACOMs and Headquarters, Department of the Army will execute in accordance with the enterprise strategy.
>
> **Goal 4 – Scale Army Knowledge Online as the enterprise portal.** Army Knowledge Online (AKO) is our integrated enterprise portal for accessing information, conducting business, and managing operations. By October 1, 2001 every Soldier – active duty, Army National Guard, and Army Reserve and Department of the Army Civilian will have an AKO account. Functional and MACOM managers must do the following two things: streamline and webify your applications; and link these applications to AKO by July 2002 or obtain a waiver from the Army CIO.
>
> **Goal 5 – Harness human capital for the knowledge organization.** The Army is People. We need to provide our military and civilian personnel with the learning opportunities, career-building tools, and mentoring relationships to improve their value to the Army and the Nation. To continuously grow our human capital, provide the Army CIO, by December 31, 2001, your innovative ideas and initiatives for reshaping our workforce into a network-centric, knowledge-based force in support of the Army civilian and military personnel management programs.[16]

The implementations of the above goals are currently underway. AKO is the first step in moving the Army to a net-centric, knowledge-based force, and is changing our information management culture. AKO provides users a universal email address, search engines, access to Army knowledge centers and functional pages, secure instant messaging and chat, news feeds, and white pages. The goal currently is to get Army personnel signed up and using this capability, which is operational today.

Strong leadership and vision for AKM points the Army in the right direction, but two of the largest problems facing the military today is our perceived lack of sharing information and the protection of our information networks. The remainder of this research paper addresses the challenges of sharing information, protecting our networks, and recommended solutions for these challenges. Goal 5 of the AKM strategic plan places emphasis on the Army professional workforce, which is our most important asset. The sharing of knowledge begins with people and it will take people to manage the knowledge of the Army.

PEOPLE AND THE CHALLENGE OF SHARING KNOWLEDGE

Before discussing people and the challenges of sharing knowledge, a few definitions are in order. The first is knowledge. "Knowledge is a fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information for decision-making."[17] There are two types of knowledge, non-recorded and recorded. Non-recorded knowledge is known as tacit knowledge or "...The personal knowledge that resides within an individual that relies on experiences, ideas, insights, values, and judgments. Knowledge that is resident within the mind, behavior, and perceptions of individuals. Knowledge developed and internalized by an individual over a long period of time incorporating so much accrued and embedded learning that its rules may be impossible to separate from how an individual acts."[18] Recorded knowledge is known as explicit knowledge or the "...Formal knowledge that can be conveyed from one person to another in systematic ways such as documents, e-mail, multimedia, etc. Knowledge that's easily codified and conveyed to others."[19]

The KM challenge is to discover and capture our tacit knowledge, share this knowledge through Army wide connectivity, and leverage explicit knowledge. If we can harness knowledge quickly, perhaps we can save the lives of many and help protect the vital interest of our nation. Consider the following fictional situation that portrays one use of KM in a tactical situation.

> The predawn silence at the U.S. Embassy in Indonesia is shattered by automatic weapons fire, and a small force of U.S. Marines barely prevents the attackers from entering the compound. Within the next few hours, the embassy sends information about the attack to the Combat Development Command in Quantico, VA. There, a team analyzes the data and sees that it matches a pattern of activity by a fundamentalist rebel group operation in the region. Another team at Quantico taps into a Community of Practice knowledge database to review new tactical maneuvers being developed in a modeling game room. Experts from across the U.S. Marine Corps join an online discussion, aided by the latest intelligence information and satellite photographs merged into an electronic workspace. Within a few hours, a new urban tactic is developed, tested in the modeling game room, and sent to the Marine commander in Indonesia. The commander coordinates plans with a U.S. Navy destroyer some 500 kilometers to the east. Later that day, he calls for fire, and 90 seconds later, the ship

> launches a dual salvo of missiles at a key rebel communications center 10 kilometers from the embassy.[20]

This fictional story shows that sharing knowledge in the military is of great importance in protecting national and military interest from our enemies. The Army can capitalize in areas from establishing better physical fitness routines, providing preventive intelligence reports, choosing the correct weapons platform to engage a target, to managing Title 10 responsibilities just by sharing and managing knowledge. Knowledge-centric organizations have become a top priority for the armed forces as high turnover, rapid rotation, and personnel cuts work to erode the military's available knowledge. The next section covers the reasons people are content with not sharing knowledge. It is a definite challenge to overcome.

THE HURDLES OF SHARING KNOWLEDGE

Everyone is looking for just the proper amount of information or knowledge to solve his or her problems. However, to gather knowledge, it has to be available. Others must be willing to share their hard-earned knowledge and insights. Unfortunately, people generally do not share their knowledge freely. Purposely or not, people believe their knowledge has value and are hesitant to share that knowledge. I believe the solution to this challenge lies in two areas, organizational culture, and process.

It is easy to change structural buildings and information networks, but when it comes to people, change becomes difficult especially when it deals with sharing knowledge in an organization. People hoard information because "knowledge is power." "While some people recognize sharing as a means for their reputation to grow, others look at the hoarding of knowledge as a means to become an "expert." If useful knowledge is held closely, then those on a knowledge search must eventually "bow at the altar" of the "hoarder." Hoarders see withholding information as a means to solidify their position in the organization; often they will not share knowledge even if asked unless they see a clear personal benefit. This approach benefits only the individual who hoards the information, usually to the detriment of the organization."[21] Another reason that people do not share knowledge falls into the area of process. In other words, are the right mechanisms in place to share information?

The process challenges fall into the area of abilities, tools, connectivity, geographical separation, access to knowledge, and trust. "If abilities or tools are not readily available to share knowledge, the process becomes too difficult to function smoothly. It may be too hard to capture or codify the knowledge. If it is not a by-product of normal work but is perceived as an additional burden, then workers will not spend the extra time on it. Connectivity must allow knowledge to be transferred to whoever needs it, when they need it, where they need it, and how they need it. Finally, it may be difficult to evaluate the quality of knowledge received. In a large organization, workers may not know each other. That lack of personal relationships makes it difficult to determine the validity and accuracy of knowledge received. If trust is not in place to support this evaluation, the work force may revert back to using only the small network of people they know and trust, which negates the power of the collective intellect of the entire organization."[22]

There is no question that organizational culture and process interferes with the smooth operation of a KM program. The Army must face head on the challenge of sharing knowledge. The following section addresses a few recommended solutions on how the Army can take on the challenges of sharing knowledge with each other.

RECOMMENDED SOLUTIONS TO PROMOTE KNOWLEDGE SHARING

Leadership from the Front

Leadership initiatives for knowledge sharing should traverse the Army both vertically and horizontally. If we allow ourselves to mire down into a strict chain of command syndrome, then knowledge sharing will lack in importance and fusion. You can not order or mandate that organizations become smart and share knowledge. Total Quality Management (TQM) was a mandate by senior leaders and the program ultimately failed within the Army. Leaders should serve as role models, encourage and reward collaborative behaviors, and provide a climate in which knowledge sharing becomes part of the normal everyday routine. A leader can influence knowledge sharing by leading from the front, caring for people, changing doctrine, training their organizations in new techniques, and providing the proper KM tools and assets to do the job with. Most important, the KM doctrine and training must start in our service schools.

The service schools for military and civilian leadership would teach the Tactics, Techniques, and Procedures (TTPs) of knowledge sharing. TTPs include incorporating good ideas (emphasis on listening), providing career-building tools (schooling, Distance Education, promotions, etc.), recruiting knowledge sharing personnel, providing funding and resources, and appointing Community of Practice (COP) leaders. Upon graduation, each leader is responsible for relaying newfound knowledge and TTPs to the schoolhouse and within the Army via COP groups or individually. Most of the TTPs are simple; the hard part is taking the time to set the example and implement it within the organization. The bottom line is that leaders need to advocate knowledge sharing within all organizations. One of the essential groups in this endeavor of change is the COP.

Community of Practice

A COP is defined as "ways people naturally work together and use technologies to create a virtual environment to electronically bring together groupings of people centered on how they work so they share knowledge."[23] The leader of the organization is responsible for appointing the COP leaders. The COP leaders are responsible for recruiting the expert knowledge participants within an organization. The leaders figure out who works together regularly because they have a job in common and then find out what they want or need to know to be more successful or to save time. Once the group is formed, they can link to other like groups outside the organization. These COPs maintain specific areas of the knowledge base. These people will become the custodians of the organization's knowledge. The leaders create sites to deposit knowledge, keep the knowledge up-to-date, and keep it fresh. Knowledge yields value when people know where it is, know how to get at it, know it will help them, keep it current, practical and useful.

The COP facilitates the exchange of successes and lessons learned and offers the opportunity to benchmark against best practices. Members will participate in developing and deploying Army wide tools, planning future projects, and testing these projects. This will build pride and ownership within the organization. Between formal meetings, the COP will be virtually connected via the Internet. The AKO Internet portal, available to all Army personnel, could facilitate the entire COP process, provide an "ask the expert" page, provide COP mailing lists, and online COP discussion group Internet chat rooms. Another important recommendation in bettering the success of knowledge sharing is mentoring.

Mentoring

Leaders, both civilian and military, can build trust and stress the importance of sharing knowledge through effective mentoring. Mentoring is defined in FM 22-100, *Army Leadership,* as "...the proactive development of each subordinate through observing, assessing, coaching, teaching, developmental counseling, and evaluating that results in people being treated with fairness and equal opportunity." Leaders need to ensure that all new personnel arriving into an organization receive a mentor. The majority of Army leaders and subordinates establish mentorship programs, but fail to follow through in the long-term relationship of mentoring. In other words, we lose touch with the people we mentor. True mentorship involves a lifetime commitment, not just a tour of duty.

A viable way for mentor and mentored to stay in touch and share knowledge is via the AKO WEB mail site. Keeping up with current phone numbers and home addresses is necessary. Senior and subordinates over the span of their careers will always learn new lessons that need sharing. This is paramount in professional and personal development. The Army mentoring process is not way off track; we just need to care more about keeping up with the people that we mentor. Another way to improve knowledge sharing within an organization is through awards and incentives.

Awards and Incentives

Current Army regulations limit what we can give to our workforce when it comes to awards and incentives. Incentive regulations differ between civilian and military and are skimpy to say the least. As leaders, we are limited to three and four-day passes for soldiers and very little money for monetary awards for civilians. We need to change the way we do business in terms of appropriate awards and incentives; it might entice our workforce to share their knowledge more freely. The idea is to reward those who contribute and derive knowledge by using the knowledge base. This will begin to remove the cultural hurdles of documenting tacit knowledge. The importance of individuals must change from what they know to how much they contribute.

Changing the Army incentive program will require thinking “out of the box,” legislative overhaul, and providing the money in the budget for better incentive awards. The structure of the program should be the same for both military and civilian. A few “out of the box” awards include paid vacations, laptop computers, savings bonds, on the spot promotions, larger monetary awards, and educational benefits. The program should clearly define the basic purpose and policy goals of incentives and the entire workforce needs to understand the program. The program should also include an effective performance monitoring and evaluation system. An excellent incentive program can contribute immensely to the way people contribute in knowledge sharing. Another way to get people to share knowledge is to provide them a capability to chat about what they know.

Chat Rooms

It is important that people collaborate with each other by using chat rooms on the AKO WEB page. Chat room communication is clear, it is in writing, it is real-time, capable of setting permissions for people to read it, and can capture knowledge and put it in a logbook. This one tool is everything KM is all about. Chat rooms provide the place to create the knowledge, use it, and transfer it, all in one simple tool. The chat room is the number one tool for leaders, COP participants, mentors, and mentored, and just plain sharers of knowledge.

All these recommended solutions require change on everyone’s part. George C. Marshall put it very clearly that an “old dog must learn new tricks.” “It became clear to me that at the age of 58 I would have to learn new tricks that were not taught in the military manuals or on the battlefield. In this position I am a political soldier and will have to put my training in rapping-out orders and making snap decisions on the back burner, and have to learn the arts of persuasion and guile. I must become an expert in a whole new set of skills."[24] Now is the time for leaders to learn the new skills of knowledge sharing, and to lead our people by setting the example.

A very important part of KM is the protection of the knowledge and systems that the knowledge resides upon. This is accomplished through a sound information assurance (IA) program. The following paragraphs address the U.S. policy on IA, assesses the adequacy of the IA policy out to 2010, covers the challenges of the policy, and points out the recommendations on how to address the challenges of the policy.

INFORMATION ASSURANCE PROTECTION, SHORTFALLS, AND RECOMMENDATIONS

"In recent years, growing concern about terrorism has led to increased attention on IA and critical infrastructure protection at the highest levels of the Federal government."[25] The DoD and the Army are developing and implementing the IA policy that is crucial in protecting our information systems. The following paragraphs address the policy and guidance of our senior leadership for IA.

SENIOR LEADERSHIP POLICY AND GUIDANCE FOR INFORMATION ASSURANCE

The Report of the President's Commission on Critical Infrastructure Protection (PCCIP), dated October 1997, emphasized the importance of protecting information systems infrastructure from attack. President Clinton signed the Presidential Decision Directive (PPD) 62 and 63 on May 22, 1998 because of the PCCIP recommendation.

At the national level, PPD 62 created the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism (NCSIPC). The NCSIPC reports to the President through the National Security Advisor and coordinates with other presidential advisors in the areas of infrastructure support issues. President Clinton reiterated his concern for the protection of the Critical Infrastructure (CI) in PDD 63 by assigning IA responsibilities. "Every department and agency CIO shall be responsible for IA."[26]

The National Security Strategy (NSS), dated January 2000, emphasizes IA. "Specific new proposals included the Federal Cyber Systems Training and Education program to offer Information Technology (IT) education in exchange for federal service; an intrusion detection network for the DoD and for federal civilian agencies; and the Institute for Information Infrastructure Protection."[27]

The President issued directives and the DoD echoed the importance of protecting our CI. The 1997 NMS listed Information Operations (IO) as an essential capability to our security. The U.S. Military must provide this key capability in order to give the national leadership a range of viable options for promoting and protecting U.S. interests in peacetime, crisis, and war. The NMS states that we must "maintain information superiority."[28] Given this strategy, the springboard for the military in the future is Joint Vision 2010.

Joint Vision 2010 articulates future operational warfighting concepts of dominant maneuver, precision engagement, full dimensional protection, and focused logistics. Each of these concepts depends on technology systems, which pass tremendous amounts of information to the warfighter. The vision states that the DoD will face Cyber attacks against our information systems, thus the need for defensive measures.

Joint Vision 2010, coupled with national and military IA policy, provides the guidance needed and are adequate to get us to 2010, but how are we doing at implementing the IA policy out to 2010? To address this question, it is important to highlight an important decision made by our senior leadership, which gave direction for implementing DoD's IA policy.

INFORMATION ASSURANCE IMPLEMENTATION AND RECOMMENDATIONS

On January 30,1998, the Deputy Secretary of Defense published a memorandum which directed the implementation of the Defense Information Assurance Program (DIAP). The DIAP's overarching mission is protecting the DoD's vital information resources by unifying and integrating IA activities to achieve information superiority. The DIAP has many IA accomplishments and a few challenges. The following paragraphs address challenges and recommendations in the areas of integration of IA policy, IA personnel resources, and IA acquisition.

Numerous U.S. IA policies exist from the national level down to our individual fighting units. Although the intent is to implement standard IA policy across DoD, there still exist overlapping, outdated, and conflicting policies. Policies exist that give too much direction and others do not provide enough.

The U.S. General Accounting Office (GAO) report to the Chairman, Committee on Armed Services, House of Representatives outlines a few of these policy challenges. "Although progress has been made in selected areas of IA policy, representatives of the IA Panel, DIAP staff and I&IA staff stated that they had not developed a strategy to ensure that the full scope of IA issues associated with DoD policies, directives, and guidance are being addressed. In addition, DIAP officials stated that they were not assessing the department wide implementation of IA policy, as assigned in the implementation plan, and had no plans to determine compliance with IA policies across DoD."[29]

To meet this challenge, the Deputy Assistant Secretary of Defense for Security and Information Operations and the GAO agreed that the OASD (C3I) IA Director should take on this challenge of policy integration. The OASD (C3I) IA Director will meet the challenge of providing a policy framework sufficient to promote sound decisions and assign roles and responsibilities of the various levels of all DoD organizations.

The next challenge is in the area of IA personnel resourcing. Significant problems exist in the area of training, retention, and management of IA personnel. Organizations acquire information networks, intrusion detection systems (IDSs), and IA tools, but do not have the proper numbers of trained IA personnel to operate the systems. Ironically, the DoD is doing more with less because of technology, but the fact is that it takes a highly skilled individual to operate these information security systems. The mind set is that automation requires fewer people, thus savings in dollars, but training these highly skilled personnel requires additional funding. Upon completion of training, the DoD quickly loses personnel to the civilian sector; thus, retention becomes a problem. The DoD cannot compete with the salaries that the civilian sector offers to our personnel. Another challenge exists in the area of personnel management. Personnel authorizations in DoD organizations have not kept up with the technology revolution; thus, not enough people to operate security systems. Many of these individuals not only operate the security systems, but also have other primary duties which distract from the importance of IA duties.

The DEPSECDEF approved the following IA personnel resource recommendations in a June 2000 Memorandum and assigned the development and implementation of the plans to the OSD staff. "Create DoD databases that track personnel with IT and IA expertise. Update TDAs and TOEs to reflect the number of personnel required to perform IA functions in an organization. Implement recruiting and retention incentives for military and civilian personnel in these specialties that compete with the civilian sector pay and incentives. Standardize criteria for education and certification of personnel performing IA functions."[30]

The last challenge for discussion is the acquisition of IA products. The largest challenge in the area of acquisition is the purchase of IA tools and products. The DoD's acquisition process is slow and cannot keep pace with the development of technology; thus the need for a new acquisition process. The DoD needs a procurement process that enables the Program Managers (PMs) of IA products to purchase new technology on demand, not five years down the road. This will ensure timely infusion of products to protect IA systems. Timeliness of fielding is important, but the certification and best quality product for a particular network is paramount.

Concurrent with the timely acquisition and fielding of the proper tools and products, PMs must provide the proper oversight of the process. This reform will require a paradigm shift in acquisition policy and training of PMs. The following paragraph is an excerpt from the DoD Chief Information Officer Annual IA Report Fiscal Year 2000, which supports the above acquisition process recommendations. "DIAP is constantly providing (or seeking to provide) IA subject matter narratives to major DoD acquisition policy modification efforts. This will enable and empower Program Managers to factor in IA requirements and costs much earlier in the acquisition life cycle of their programs. In concert with this effort, they will seek participation with J8/JCS to provide the appropriate forum for the development and refinement of IA doctrine as it applies to acquisition. The Acquisition Group will continually interface with other DIAP functional groups to help promote Research and Development transition, Architecture transition, Modeling and Simulation development, Test and Evaluation incorporation, Training definition, and Logistics transition."[31]

CONCLUDING REMARKS

It is true that the Army and DoD have challenges in the area of information technology and knowledge sharing. The good news is that the senior leadership has set into motion a plan of transformation to address these challenges. A simple but well-coordinated and communicated vision brought the Signal Corps C4 community to proactively address the challenges of transformation. The vision will move us from the legacy to the objective force with the Secretary of the Army and CSA leading the way. It is essential that we move out of the "Stone Age" of current day information exchange to AKM. AKM is the center pole in the tent for Army transformation and will change our culture and the way we do business in the Army. We are ridding ourselves of traditional practices and moving toward teamwork and innovation. The challenges ahead are real and will take a concerted effort by all to share knowledge amongst the entire force. KM will ensure that the right information arrives at the right time, in the right form, assured and secure, to the right person or people. Leadership, COPs, mentoring, awards, incentives, and chat rooms are just a few important ways to implement knowledge sharing in any organization.

The Cyber threat is real throughout the world and the DoD can expect future attacks on crucial information systems that provide command and control, support operational missions, and provide management functions. The DoD has sufficient IA policy in place to ensure the protection of information systems out to the year 2010. Although challenges exist in the areas of policy integration, personnel resources, and acquisition, sound recommendations are in place and have been set in motion by the appropriate leadership in DoD. Since 1997, the DoD has come a long way in protecting information systems but can never become complacent in improving IA against a never-ending threat. The 2001 Quadrennial Defense Review Report reiterates the importance of IA. "Assure information systems in the face of attack and conduct effective information operations."[32]

The Army is on a journey towards transformation. AKM and assured information systems are essential enablers of this transformation, which will move the Army to the objective force. Challenges exist, but that never stopped the Army from accomplishing the mission. People will address the challenges and implement solutions to overcome the hurdles.

> "Moving our Army into the next century is a journey, not a destination; we know where we are going and we are moving out."
>
> General Gordon R. Sullivan
> Chief of Staff, U.S. Army

WORD COUNT = 7,466

ENDNOTES

[1] John M. Shalikashvili, Joint Vision 2010, (Washington, D.C.: U.S. Department of Defense, 1996), 16.

[2] John M. Shalikashvili, The 1997 National Military Strategy of the United States-Shape, Respond, Prepare Now: A Military Strategy for a New Era, (Washington, D.C.: U.S. Department of Defense, September 1997), 18.

[3] Henry H. Shelton, Joint Vision 2020, (Washington, D.C.: U.S. Department of Defense, June 2000), 8.

[4] Donald H. Rumsfeld, Quadrennial Defense Review Report, (Washington, D.C.: U.S. Department of Defense, September 2001), 46.

[5] Ibid, 54.

[6] David S. Alberts, John J. Garstka, and Frderick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority 2nd Edition (Revised), (Washington, D.C.: DoD C4ISR Cooperative Research Program, 2000), 1.

[7] Ibid, 46-48.

[8] Department of the Army, Transformation Campaign Plan, U.S. Army War College Selected Readings, Academic Year 2002, Course 1 Strategic Leadership Volume II (Carlisle Barracks: U.S. Army War College, 31 July – 21 August 2001), 178.

[9] Department of the Army, Army Knowledge Management Strategic Plan Version 2.1, (Washington, D.C.: Director of Information Systems for Command, Control, Communications, and Computers, 8 August 2001), 59.

[10] LTG Peter M. Cuviello, "DISC4 Vision and Goals," memorandum for DISC4, Washington, D.C., July 2001.

[11] Department of the Army, Army Knowledge Management Strategic Plan Version 2.1,17.

[12] LTG Peter M. Cuviello, "Army Knowledge Management Briefing for Army Strategic Leadership Course," briefing slides, Washington D.C., 19 June 2001.

[13] Ibid.

[14] Department of the Army, Army Knowledge Management Strategic Plan Version 2.1, 11.

[15] Secretary of the Army Thomas E. White and Chief of Staff of the Army General Eric K. Shinseki, "Army Knowledge Management Guidance Memorandum Number 1," memorandum for see distribution, Washington, D.C., 8 August 2001.

[16] Ibid.

[17] Department of the Army, Army Knowledge Management Strategic Plan Version 2.1, 52.

[18] Ibid, 55.

[19] Ibid, 50.

[20] Gary H. Anthes, "Charting a Knowledge Management Course," COMPUTERWORLD August 2000; available from <http://www.computerworld.com/cwi/story/0,1199,NAV47_STOR48722,00.html>; Internet; accessed 20 November 2001.

[21] George Cho, Hans Jerrell, and William Landay, Program Management 2000: Know The Way, Report of the Military Research Fellows DSMC 1998-1999 (Fort Belvoir: Defense Systems Management College, January 2000), 3-3.

[22] Ibid, 3-3 – 3-4.

[23] Department of the Army, Army Knowledge Management Strategic Plan Version 2.1, 54.

[24] Department of Command, Leadership, and Management, Strategic Leadership Primer, (Carlisle Barracks: U.S. Army War College, 1998), 1.

[25] John L. Woodward, JR., INFORMATION ASSURANCE, Legal, Regulatory, Policy and Organizational Considerations, 4th Edition (2nd Printing), (Washington D.C.: U.S. Department of Defense, August 1999), ES-1.

[26] William J. Clinton, PPD 63: The Clinton Administration's Policy on Critical Infrastructure Protection, (Washington D.C.: The White House, 1998), 6.

[27] William J. Clinton, A National Security Strategy For A Global Age, (Washington D.C.: The White House, December 2000), 24.

[28] Shalikashvili, 27.

[29] General Accounting Office, INFORMATION SECURITY Progress and Challenges to an Effective Defense-wide Information Assurance Program (Washington, D.C.: U.S. General Accounting Office, March 2001), 18.

[30] Arthur L. Money, Annual Information Assurance Report Fiscal Year 2000, (Washington D.C.: U.S. Department of Defense, 2000), 35.

[31] Ibid., 57.

[32] Rumsfeld, 43.

BIBLIOGRAPHY

Alberts, David S., Garstka, John J., and Stein, Frderick P. Network Centric Warfare: Developing and Leveraging Information Superiority 2nd Edition (Revised). Washington D.C.: DoD C4ISR Cooperative Research Program, 2000.

Alliance, Athena and Jarboe, Kenan Patrick. Knowledge Management As an Economic Development Strategy. Reviews of Economic Development Literature and Practice: No. 7. Washington D.C.: U.S. Economic Development Administration, April 2001.

Ambrosio, Johanna. "Knowledge Management Mistakes." COMPUTERWORLD 3 July 2000. Available from <http://www.computerworld.com/cwi/story/0,1199,NAV47_STO46693,00.html>. Internet. Accessed 20 November 2001.

Anthes, Gary H. "Charting a Knowledge Management Course." COMPUTERWORLD 21 August 2000. Available from <http://www.computerworld.com/cwi/story/0,1199,NAV47_STO48722,00.html>. Internet. Accessed 20 November 2001.

Battery, Jim. "Governing with e-speed." InfoWorld 23 March 2001. Available from <http://www.infoworld.com/articles/ca/xm1/01/03/26/010326cagovt.xml>. Internet. Accessed 20 November 2001.

Bennet, Alex. "Knowledge Management: Unlocking the Potential of Our Intellectual Capital." June 1999. Available from <http://www.chips.navy.mil/archives/00_jan/km.htm>. Internet. Accessed 30 November 2001.

Berkman, Eric. "When Bad Things Happen to Good Ideas." Darwin Online April 2001. Available from <http://www.darwinmag.com/read/040101/badthings_content.html>. Internet. Accessed 20 November 2001.

Castro, Felix D. Jr. Integrating Knowledge Management Initiatives for the Future Army. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 18 September 2000.

Cho, George, Jerrell, Hans, and Landay, William. Program Management 2000: Know The Way. Report of the Military Research Fellows DSMC 1998-1999. Fort Belvoir: Defense Systems Management College, January 2000.

Clinton, William J. A National Security Strategy For A Global Age. Washington, D.C.: The White House, December 2000.

_________. PPD 62: The Clinton Administration's Policy on Critical Infrastructure Protection. Washington, D.C.: The White House, May 1998.

_________. PPD 63: The Clinton Administration's Policy on Critical Infrastructure Protection. Washington, D.C.: The White House, May 1998.

Cortright, Joseph. New Growth Theory, Technology and Learning: A Practitioners Guide. Reviews of Economic Development Literature and Practice: No. 4. Washington D.C.: U.S. Economic Development Administration, 2001.

Curley, Kathy. "10 Myths About Knowledge Management." COMPUTERWORLD 4 January 2001. Available from <http://www.computerworld.com/cwi/story/0,1199,NAV47_STO55870,00.html>. Internet. Accessed 20 November 2001.

Cuviello, Peter M. "Army Knowledge Management Briefing for Army Strategic Leadership Course." Briefing slides, Washington D.C., 19 June 2001.

________. "DISC4 Vision and Goals." Memorandum for DISC4. Washington D.C., July 2001.

________. <peter.cuviello@hqda.army.mil>, "DISC4 AKO accounts." Electronic mail message to DISC4 Civilians, DISC4 Contractors, and DISC4 Military. 6 August 2001.

Davenport, Thomas H. "Successful Knowledge Management Projects." Sloan Management Review Winter 1998. Available from <http://www.findarticles.com/cf_dls/m4385/n2_v39/20390224/print.jhtml>. Internet. Accessed 11 December 2001.

Department of Command, Leadership, and Management. Strategic Leadership Primer. Carlisle Barracks: U.S. Army War College, 1998.

Department of Command, Leadership, and Management. Managing Strategic Change: An Executive Overview of Management (Final Draft). Carlisle Barracks: U.S. Army War College, 2001.

Desenberg, Jon. "Moving Past the Information Age: Getting Started with Knowledge Management." IMP magazine information IMPACTS July 2000. Available from <http://www.cisp.org/imp/july_2000/07_00desenberg.htm>. Internet. Accessed 20 November 2001.

Dyer, Greg and McDonough, Brian. "The State of KM." Destination CRM KNOWLEDGE MANAGEMENT May 2001. Available from <http://www.destinationcrm.com/km/dcrm_km_article.asp?id=822&ed=5%2F1%2F01>. Internet. Accessed 20 November 2001.

Eisenhart, Mary. "Washington's Need to Know." Destination CRM KNOWLEDGE MANAGEMENT May 2001. Available from <http://www.destinationcrm.com/km/dcrm_km_article.asp?id=658>. Internet. Accessed 20 November 2001.

Figura, Susannah Zak. "Human Capital: The Missing Link." Government Executive Magazine 1 March 2000. Available from <http://www.govexec.com/gpp/0300hr.htm>. Internet. Accessed 20 November 2001.

Fore, Donna, Johns, Sonja, Luoma, Marc, and Shalak Michael. Knowledge Warrior for the 21st Century Catalysts for Cultural Change. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 18 September 2000.

Harris, Shane. "Daniels creates e-government task force." Government Executive Magazine 23 July 2001. Available from <http://www.govexec.com/dailyfed/0701/072301s1.htm>. Internet. Accessed 20 November 2001.

Kotter, John P. Leading Change. Harvard Business School Press, 1996.

McClintock, Bruce H. “Transformation Trinity Vision, Culture, Assessment.” Joint Force Quarterly JFQ, Autumn 2000, 27-31.

Money, Arthur L. Annual Information Assurance Report Fiscal Year 2000. Washington, D.C.: U.S. Department of Defense, 2000.

O’hanlon, Michael. Technological Change and the Future of Warfare. Brookings Institution Press, 2000.

Osterholz, John. “Implementation of the Global Information Grid.” Briefing slides. Carlisle Barracks: U.S. Army War College, 5 December 2001.

Penny, Paul. “Knowledge Management: Maximizing the Return on Your Intellectual Assets.” DM Review 20 November 2001. Available from <http://www.dmreview.com/portal_ros.cfm?NavID=91&EdID=2678&PortalID=17>. Internet. Accessed 20 November 2001.

Rumsfeld, Donald H. Quadrennial Defense Review Report. Washington, D.C.: U.S. Department of Defense, September 2001.

Shalikashvili, John M. Joint Vision 2010. Washington, D.C.: U.S. Department of Defense, 1996.

_________. The 1997 National Military Strategy of the United States-Shape, Respond, Prepare Now: A Military Strategy for a New Era. Washington, D.C.: U.S. Department of Defense, September 1997.

Shein, Esther. “The Knowledge Crunch.” CIO Magazine 1 May 2001. Available from <http://www.cio.com/archive/050101/crunch_content.html>. Internet. Accessed 20 November 2001.

Shelton, Henry H. Joint Doctrine for Information Operations, Joint Publication 3-13. Washington D.C.: U.S. Department of Defense, 9 October 1998.

_________. Joint Vision 2020. Washington, D.C.: U.S. Department of Defense, June 2000.

Sviokla, John. “Knowledge Pays.” CIO Magazine 15 February 2001. Available from <http://www.cio.com/archive/021501/new_content.html?printversion=yes>. Internet. Accessed 20 November 2001.

Tang, Beth Archibald. “Knowledge management is power.” Federal Computer Week 15 February 2001. Available from <http://www.fcw.com/fcw/articles/2001/0212/web-dotgov-02-15-01.asp>. Internet. Accessed 20 November 2001.

U.S. Department of the Army. Army Knowledge Management Strategic Plan Version 2.1. Washington, D.C.: Director of Information Systems for Command, Control, Communications, and Computers, 11 June 2001.

U.S. Department of Commerce Economic Development Administration. Evaluating Business Development Incentives. Washington D.C.: U.S. Department of Commerce Economic Development Administration, August 1999.

________. Transformation Campaign Plan. U.S. Army War College Selected Readings, Academic Year 2002, Course 1 Strategic Leadership Volume II. Carlisle Barracks: U.S. Army War College, 31 July – 21 August 2001.

U.S. General Accounting Office. INFORMATION SECURITY Progress and Challenges to an Effective Defense-wide Information Assurance Program. Washington, D.C. U.S. General Accounting Office, March 2001.

Weidner, Douglas. "Knowledge Management Choosing the Best IM Initiative." E-Gov Journal 4 November 2000. Available from <http://www.e-gov.com/egovjournal/neews/index.pl?article=77&dept=oped>. Internet. Accessed 20 November 2001.

White, Thomas E., Secretary of the Army. "Army Knowledge Management Guidance Memorandum Number 1," Memorandum for See Distribution. Washington, D.C., 8 August 2001.

Woodward, John L. JR. INFORMATION ASSURANCE, Legal, Regulatory, Policy and Organizational Considerations, 4th Edition (2nd Printing). Washington D.C.: U.S. Department of Defense, August 1999.